Application: _____

Exhibit No.: SDG&E-_____

PREPARED DIRECT TESTIMONY OF

CHRISTOPHER VERA

ON BEHALF OF SAN DIEGO GAS & ELECTRIC COMPANY

CHAPTER 4

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

November 26, 2018

TABLE OF CONTENTS

I. INTRODUCTION 1

II. SDG&E'S RESPONSIBILITY TO SAFEGUARD CUSTOMER PRIVACY 1

III. EXAMPLES OF MISUSE OF UTILITY SYSTEMS AND CUSTOMER INFORMATION IN DEMAND RESPONSE 3

IV. INDUSTRY STANDARDS SUPPORT SDG&E VALUES: CUSTOMER PRIVACY, CHOICE, INFORMED CONSENT 5

V. THE ALTERNATE SOLUTION'S PRIVACY RISKS AND IMPLICATIONS 6

A. Brief description of the Alternate Solution 6

B. The Alternate Solution Poses Privacy Risks 6

C. Consequences 10

VI. CONCLUSION 11

VII. STATEMENT OF QUALIFICATIONS 12

LIST OF ACRONYMS 13

PREPARED DIRECT TESTIMONY OF CHRISTOPHER VERA CHAPTER 4

I. INTRODUCTION

The purpose of my prepared direct testimony is to describe San Diego Gas & Electric Company's ("SDG&E") privacy concerns regarding Solution 1b (also referred to in this application as the "Alternate Solution"), including SDG&E's responsibility to safeguard customer privacy, the privacy risks and implications of Solution 1b, and SDG&E's recommendations for preserving customer privacy while making it as convenient as possible for customers to provide their consent to enable third parties to efficiently receive their utility data. While this testimony focuses on privacy risks related to Solution 1b, it must be noted that these same risks apply equally if not more so to Solution 1a.[1]

II. SDG&E'S RESPONSIBILITY TO SAFEGUARD CUSTOMER PRIVACY

In 2011, recognizing that energy usage data would fast become an asset collected by utilities and highly coveted by a myriad of third parties seeking access to this information for financial benefit, the State of California and the California Public Utilities Commission ("Commission" or "CPUC") established a robust collection of privacy rules that Investor-Owned Utilities ("IOU") are required to follow. The Commission's "Decision ["D."] Adopting Rules to Protect the Privacy and Security of the Electric Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company,"[2] informally referred to as the "Smart Grid Privacy Decision," "adopts rules to protect

---

[1] The Prepared Direct Testimony of Claudio Pellegrini (Chapter 3) ("Pellegrini Testimony") discusses the differences between Solution 1a and Solution 1b and the information technology and security considerations and concerns associated with those two proposals.

[2] *See* D.11-07-056.

the privacy and security of customer data generated by Smart Meters" and "policies to govern access to customer usage data by customers and by authorized third parties."[3] The Smart Grid Privacy Decision was later expanded to cover gas usage data, and data collected by gas utilities and Community Choice Aggregators ("CCAs").[4]

These rules further align with and support Public Utilities Code ("PUC") section ("§") 8380, which directs California energy corporations not to "share, disclose, or otherwise make accessible to any third party a customer's electrical or gas consumption data, except as provided in subdivision (e) or upon the consent of the customer."[5] PUC section 8380 further requires energy corporations to "use reasonable security procedures and practices to protect a customer's … consumption data from unauthorized access, destruction, use, modification, or disclosure."[6]

In June 2018, the State of California passed the Consumer Privacy Act of 2018 ("CCPA"), which goes into effect January 1, 2020.[7] This new law introduces sweeping privacy requirements for companies that collect, sell or share customer data. While the full impacts of the law are still being assessed by legal advisors around the state and regulations remain to be issued by the California Attorney General, the law affords consumers "the right to request that a business that collects a consumer's personal information disclose to that consumer" the information the company has collected,[8] and, subject to exceptions, to "request that a business

---

[3] *Id.*, p. 2.

[4] *See* D.12-08-045.

[5] PUC § 8380(b)(1).

[6] *Id.*, § 8380(d).

[7] Assembly Bill ("AB") 375, Stats. 2017-2018, Ch. 55 (Cal. 2018) and Senate Bill ("SB") 1121, Stats. 2017-2018, Ch. 735 (Cal. 2018).

[8] *Id.*, § 1798.100(a).

delete any personal information about the consumer which the business has collected from the consumer."[9] Further, the law subjects companies who fail to "maintain reasonable security procedures and practices," to the potentially significant financial penalties.[10]

These privacy mandates have a direct effect on business decisions made by SDG&E when it comes to preserving customer privacy and sharing customer information with third parties. While SDG&E recognizes the value in making it easier to obtain customer consent, compliance with existing privacy law and regulation must be a principle concern when contemplating solutions for the click-through authorization process ("CTP").

The goal of the CTP is to make it easy and secure for customers to provide—and when necessary, to revoke— their consent to share data, usually in regard to participation in a third-party program of their choice, while preserving their privacy. For the technical and security-related reasons described in Mr. Claudio Pellegrini's testimony (Chapter 3),[11] SDG&E concludes that the Alternate Solution does not meet the industry standards and requirements contained in State law and the Commission's Smart Grid Privacy Decision and may result in the unintended consequence of abuse by bad actors who seek to obtain and misuse customer information at any price.

III. EXAMPLES OF MISUSE OF UTILITY SYSTEMS AND CUSTOMER INFORMATION IN DEMAND RESPONSE

Concerns for the potential of third-party abuse or misuse of utility customer information is not unfounded. Even where customer privacy protections exist, third parties have obtained

---

[9] *Id.,* § 1798.105(a).

[10] *Id.*, § 1798.150(a)(1).

[11] *See* Pellegrini Testimony, Section VIII. Cost Estimate for Alternate Solution (OP 29, Bullet #2).

and used confidential customer data to meet their own objectives rather than the customer's intended use. A few examples include:

1. Known third-party violations.

In March 2017, SDG&E reported evidence of "screen scraping" practices to the CPUC in which at least one demand response provider ("DRP") collected MyAccount[12] usernames and passwords from SDG&E customers in violation of SDG&E's MyAccount terms and conditions for purposes of automatically logging into these customers' MyAccount to obtain their contact information, energy usage and related account data using automated software (*i.e.*, "screen scraping"). Beginning in June 2016, at least one other IOU also reported similar activity to the CPUC by a third-party DRP whose actions adversely impacted that utility's systems.

2. Industry observations of misuse.

Nest, a manufacturer of smart thermostats, warns its customers of similar third-party "screen scraping" behavior on their website, which states: "Companies that are not certified Works With Nest partners may ask you to use your account information to sign into their service. Other websites or apps may try to simply steal your account email and password by posing as a Works With Nest partner. Sharing your account email and password with unauthorized websites or apps can compromise the security of your home and personal information."[13]

---

[12] MyAccount is described in the Prepared Direct Testimony of Tishmari Lewis (Chapter 2), Section V. Whitepaper Response: Requests for Additional Data – Not Recommended.

[13] Nest, *Nest Support, Don't Share Your Account Email and Password*, *available at* https://nest.com/support/article/sharing-your-nest-account-email-and-password-with-other-companies-advertising-compatibility-with-nest, as of October 2018.

3. Non-utility observations of misuse.

The recent Facebook data breach[14] involving third-party Cambria Analytics clearly demonstrates the risks posed by choosing convenient third-party access to customer data over reasonable standards-based security and privacy controls. Facebook provided access to sensitive customer data to a third-party researcher who in turn used this information for its own purposes. This led to an inquiry by the Federal Trade Commission, Congressional hearings, and massive backlash from Facebook users. The effects of this breach are still being felt today, particularly in the State of California, and this significant event was one of several that led to the drafting of the CCPA.

IV. INDUSTRY STANDARDS SUPPORT SDG&E VALUES: CUSTOMER PRIVACY, CHOICE, INFORMED CONSENT

To counter both inadvertent and intentional threats to customer privacy, SDG&E advocates for industry-standard practices and technologies that are proven to have withstood the test of time and testing by security professionals to ensure these practices are working effectively. This is preferred over solutions that may appear convenient at the moment but too often result in the unauthorized use or acquisition of customer information, loss of customer trust, and possible violation of California law and Commission privacy regulations.

SDG&E subscribes to the use of standards-based best practices when it comes to securing customer data. The Open Authorization standard ("OAuth"),[15] described in Mr. Pellegrini's testimony (Chapter 3), and similar industry Internet standards, are open (meaning accessible and

---

[14] CNBC, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal* (April 10, 2018), *available at* https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html, as of October 2018.

[15] Internet Engineering Task Force, *The OAuth 2.0 Authorization Framework, RFC 6749* (October 2012), *available at* https://datatracker.ietf.org/doc/rfc6749/.

reproducible for use by companies like SDG&E) and widely used to reasonably ensure that the customer and no other has made an informed decision to consent to sharing their personal information during the CTP. Further, when using OAuth protocols, the customer cannot repudiate whether this action has occurred. If consent was given, all parties can be reasonably confident the customer indisputably provided it. This protects the third-party, the utility, as well as the customer.

V. THE ALTERNATE SOLUTION'S PRIVACY RISKS AND IMPLICATIONS

A. Brief description of the Alternate Solution

A detailed description of the technical aspects and technical security risks posed by the Alternate Solution can be found in Mr. Pellegrini's testimony (Chapter 3).[16] The Alternate Solution is a non-standard solution that requires critical customer authentication and authorization functions to move or pass through a non-trusted third party's infrastructure rather than remain within the trusted boundary of the utility. In a layperson's terms, this is roughly equivalent to a customer disclosing their debit card PIN number to a cashier, so the cashier can complete a sale. This testimony will discuss the privacy implications of these security compromises.

B. The Alternate Solution Poses Privacy Risks

There are several privacy risks related to the Alternate Solution, which are described below.

Inability to reasonably identify the customer. The Alternate Solution requires the third-party to collect and share the necessary contact information about the customer to properly authenticate them. This contact information generally includes information that many people

[16] *See* Pellegrini Testimony, Section VIII. Cost Estimate for Alternate Solution (OP 29, Bullet #2).

besides the customer may know (such as email address and phone numbers) and excludes information that is generally known only to the customer (such as their MyAccount credentials, account number, or portion of their social security number, which is common on many secure websites involving the transacting of sensitive customer information). It is impossible for the utility to positively determine whether the information being provided is directly from the customer rather than the third-party or a malicious "man in the middle" who has compromised the transaction. This represents significant risk in positively identifying and authenticating the customer. Solution 1b's inclusion of a "two-factor" authentication (*i.e.*, requiring a code be generated and sent to the customer's email address or phone number) slightly reduces this risk but does not reasonably minimize it because the transaction requires accurate contact information previously provided by the customer to the utility to reliably complete the process. Outdated contact information could result in two-factor challenges not being delivered to the customer, or worse, to a party not involved at all in the transaction. Therefore, the Alternate Solution's privacy risk begins with a lack of reasonable trust that the utility on the downstream end of the process is interacting with the actual customer of record.

Lack of trust in proposed authorization. This privacy concern has to do with authorization, or the confirmation of what data the customer specifically intends to grant the utility permission to share with the third-party. In addition to collecting the customer's data as stated above, the Alternate Solution dictates that the third-party will also take responsibility for securing the customer's authorization (including details about what customer data the customer consents to share, such as meters, accounts, timeframes of authorization, etc.), which are critical components of the consent contract. If we assume momentarily that we had positively identified and authenticated the customer, despite the significant obstacles described above, the utility still

would have no way to determine whether the customer's actual intent was being accurately conveyed to it by the third-party. Aggressive third parties, malicious actors acting as a "man in the middle," and even innocent third parties who have misconfigured their systems, could misrepresent what data the customer intended to share with the third-party. Under the Alternate Solution proposed, the utility would have no choice but to rely on this authorization as accurate and truthful without any reasonable validation by the customer.

Repudiation of customer consent. Because of the issues created by the Alternate Solution's authentication and authorization mechanisms, another problem is introduced: The absence of non-repudiation. Although both the third-party and SDG&E can log that a transaction took place, given the weakness in the aforementioned security controls, it is reasonably possible for a customer to deny that they were the party who authorized the specific consent transaction and neither the third-party nor the utility would have any reasonable means to disprove such an accusation. This would likely result in SDG&E being blamed for sharing a customer's energy usage (or other) data without proper authorization, potentially resulting in a reportable security incident per D.11-07-056.

Lack of security auditing controls. While the Commission can order utilities to implement specific security controls, such as auditing and logging, the third parties wishing to utilize the Alternate Solution answer to no comparable regulatory body. This means the inclusion of critical auditing controls in the Alternate Solution to determine what took place during the transaction should errors or illicit activity occur is dependent entirely on the third party's whim to include such controls, and such controls could be removed or disabled at any time if they are implemented at all. Further, it is unclear whether third parties will use uniform standards in customer privacy and information security controls or be transparent regarding their

existing safeguards. While some third parties may do well at protecting customer information and auditing transactions, others may not adhere to even fundamental security requirements. Unfortunately, because there are no audit requirements or accountability measures for privacy and security by participating third parties, there is no way to tell the difference until after a security incident has occurred and even then, there is no mandate or incentive for poor-performing third parties to conform to any set of privacy, security or auditing standards. This lack of formal accountability and auditing validation inflates the risks introduced by the Alternate Solution, and potentially and inappropriately transfers this increased risk to ratepayers, whose utilities do have such obligations. This contrasts with the current CTP in which the utility manages necessary security logging.

Difficulty with customer revocation of consent. Even assuming all other risks have been mitigated, a path for customer revocation remains unclear. While Resolution E-4868 ("Resolution") contemplates customer consent that "begins and ends on a third-party website,"[17] there is no such direction for revocation, which is a fundamental customer right. Customer revocation should be as easy to invoke as it was to provide consent in the first place. Solution 1b does not provide the customer any clear process to revoke their consent once granted and may confuse participating customers who have not directly interacted with the utility during the 1b process as to what they must do to revoke their consent should they so choose. Compare this to the existing CTP in which customers grant and revoke consent in the same place.

New legal risks. With enactment of the CCPA, California companies that meet specific criteria, including the California IOUs, will need to apply stringent new privacy standards regarding customer reporting and, subject to exceptions, data deletion beginning in January

[17] Resolution, p. 5.

2020. The impact of these new privacy requirements on utility data sharing transactions remains unclear. While the effects of this new law are not unique to the Alternate Solution, the lack of non-standard authentication, authorization, accountability, and non-repudiation controls introduced by the Alternate Solution could run afoul of the utilities' need to maintain reasonable security practices. SDG&E expresses its concern that the Alternate Solution may not be considered a "reasonable" security practice according to industry standards or the new law.

C. Consequences

The privacy risks discussed above result in the following consequences:

There will be a lack of utility standards-based trust. Utilities will have little confidence in whether the actual customer of record has authenticated into the process, and authorized their consent, or whether someone else impersonated them using information they know about the customer. Nor will the utility or the customer be able to trust that the authorization ostensibly received from the third-party is the customer's stated intent as there is no way to validate the scope of what the customer authorized against what the third-party conveyed to the utility.

Consequently, some risks may be inappropriately transferred to utilities. Because of the repudiation risks, customers will question the utility—not the third-party—when they believe they did not consent to sharing their information with a third-party. The utility will have been left with no ability to refute such claims.

There is also a lack of adequate security auditing. Neither the utility nor the Commission will have any record of what happened in the event a transaction error occurs, or the process is targeted by illicit behavior. Neither will the utility have the ability to hold third parties accountable to industry-standard privacy and security practices if their security auditing controls prove inadequate or non-existent. This consequence will make it difficult for the Commission to investigate complaints against third parties by customers, as allowed under Rule 32.

Customers will have no clear path to revoke consent. In addition to existing Commission privacy requirements, potential new legal liabilities require IOUs to evaluate their data sharing processes for reasonable security practices in order to minimize risk. The CCPA introduces new privacy requirements that may adversely impact utilities that use non-standard security practices to share sensitive customer data with third parties.

VI. CONCLUSION

As demonstrated by my prepared direct testimony, the legal and privacy concerns raised by the Alternate Solution cannot be adequately mitigated. To avoid these concerns, SDG&E recommends the Commission reject the Alternate Solution and instead continue with the current CTP.

This concludes my prepared direct testimony.

VII. STATEMENT OF QUALIFICATIONS

My name is Christopher Vera. I am employed by SDG&E as its manager of Office of Customer Privacy ("OCP"). My current responsibilities include overseeing SDG&E's customer privacy program, including compliance with California privacy law and Commission regulations affecting customer privacy. I assumed my current position in 2012. I have been employed by SDG&E since 2002 in its Information Security department and have held positions of increasing authority until assuming the role of OCP Manager. I am/was the lead author of the Cyber Security and Privacy section of SDG&E's 2012 Smart Grid Deployment Plan.

I have over 20 years' experience in the information and cyber security industry, including the development and management of several programs for the defense and energy sectors, including: incident response and e-forensics, vulnerability management, and security awareness and training, as well as the development of strategies, architectures, policies, standards and procedures for privacy and security compliance and governance programs. I am a Certified Information Systems Security Practitioner ("CISSP") and a member of the International Association of Privacy Professionals ("IAPP").

I have not previously testified before the Commission.

LIST OF ACRONYMS

AB	Assembly Bill
CCAs	Community Choice Aggregators
CCPA	California Consumer Privacy Act
CISSP	Certified Information Systems Security Practitioner
CPUC	California Public Utility Commission
CTP	Click-Through Authorization Processes
D.	Decision
DRP	Demand Response Provider
IAPP	International Association of Privacy Professionals
IOU	Investor-Owned Utilities
PUC	Public Utilities Code
SB	Senate Bill
SDG&E	San Diego Gas & Electric Company